Universität Heidelberg
Mathematisches Institut
Sommersemester 2022

Prof. Dr. Otmar Venjakob
Milan Malčić
Heidelberg, 24. Juni 2022

Lineare Algebra II

Übungsblatt 9

Aufgabe 1. (1+1.5+1.5 Punkte). Sei R ein euklidischer Ring und $a, b \in R \backslash \{0\}$. In dieser Aufgabe beschreiben wir den *Euklidischen Algorithmus* zur Berechnung von $\mathrm{ggT}(a, b)$. Durch sukzessive Division mit Rest erhalten wir

$$\begin{aligned} a &= q_0 b + r_0 && (0) \\ b &= q_1 r_0 + r_1 && (1) \\ r_0 &= q_2 r_1 + r_2 && (2) \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n && (n) \\ r_{n-1} &= q_{n+1} r_n + 0. && (n+1) \end{aligned}$$

Dabei ist r_n der letzte Rest, der ungleich Null ist. Ein solches $n \in \mathbb{N}$, für das der Rest r_{n+1} gleich Null ist, existiert tatsächlich, denn $\delta(b) > \delta(r_0) > \delta(r_1) > \ldots > \delta(r_n)$ ist -- solange die Reste r_i ungleich Null sind -- eine streng monoton fallende Folge natürlicher Zahlen, und so eine Folge muss abbrechen.

a) *Zeigen Sie*: Es ist (bis auf Assoziiertheit) $r_n = \mathrm{ggT}(a, b)$.

Als Nächstes erklären wir, wie der Euklidische Algorithmus eine explizite Darstellung von $\mathrm{ggT}(a, b)$ als Linearkombination $\mathrm{ggT}(a, b) = xa + by$ in a und b liefert: Aus Gleichung (n) erhält man eine Darstellung von $\mathrm{ggT}(a, b) = r_n$ als Linearkombination in r_{n-2}, r_{n-1}, unter Hinzunahme von Gleichung $(n-1)$ als Linearkombination in r_{n-3}, r_{n-2} usw., bis schließlich $\mathrm{ggT}(a, b)$ unter Benutzung von Gleichung (0) als Linearkombination in a und b dargestellt ist.

b) Sei $R = \mathbb{Z}, a = 1891, b = 3797$. *Berechnen Sie* $\mathrm{ggT}(a, b)$ und stellen Sie ihn als Linearkombination in a und b dar. Entscheiden Sie mit dieser Information, ob die Restklasse $\overline{a}$ eine Einheit in $\mathbb{Z}/b\mathbb{Z}$ ist und geben Sie ggf. das multiplikative Inverse $\overline{a}^{-1}$ an.

b) Sei $R = \mathbb{Q}[X], a = X^6 - X^5 + 6X^2 - 13X + 7, b = X^3 + X^2 + X - 3$. *Berechnen Sie* $\mathrm{ggT}(a, b)$ und entscheiden Sie mit dieser Information, ob die Restklasse von a eine Einheit in $R/(b)$ ist.

Aufgabe 2. $(2 + 1 + 1$ Punkte). Wir betrachten den Unterring

$$\mathbb{Q}[i\sqrt{5}] := \{a + b \cdot i\sqrt{5} \mid a, b \in \mathbb{Q}\}$$

von $\mathbb{C}$.

a) *Zeigen Sie*: $\mathbb{Q}[i\sqrt{5}]$ ist isomorph zu $\mathbb{Q}[X]/(X^2 + 5)$ und auch zu $\mathbb{Q}[X]/(X^2 - 2X + 6)$.

b) *Folgern Sie* aus a): $\mathbb{Q}[i\sqrt{5}]$ ist ein Körper.

c) Sei $a + bX \in \mathbb{Q}[X] \setminus \{0\}$. *Finden Sie* $f, g \in \mathbb{Q}[X]$ mit $f \cdot (a + bX) + g \cdot (X^2 + 5) = 1$. Berechnen Sie mit dieser Information das multiplikative Inverse von $a + b \cdot i\sqrt{5}$ in $\mathbb{Q}[i\sqrt{5}]$.

Abgabe bis Freitag, 01. Juli 2022, 11 Uhr in die Zettelkästen vor dem Dekanat (Mathematikon, INF 205, 1. Stock) oder online via MaMpf

Aufgabe 3. ($1 + 1 + 1 + 1$ Punkte). Sei R ein kommutativer Ring und seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise koprime Ideale, d.h. für die Summe $\mathfrak{a}_i + \mathfrak{a}_j := \{a + b \mid a \in \mathfrak{a}_i, b \in \mathfrak{a}_j\}$ gilt $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$. Sei $\pi_i \colon R \to R/\mathfrak{a}_i$ jeweils die kanonische Projektion. Wir betrachten den Ringhomomorphismus

$$\varphi \colon R \to R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n, \qquad x \mapsto (\pi_1(x), \ldots, \pi_n(x)).$$

In dieser Aufgabe möchten wir den *Chinesischen Restsatz* beweisen, welcher besagt, dass φ surjektiv ist und $\ker(\varphi) = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$ erfüllt, also einen Isomorphismus

$$R/\bigcap_{i=1}^{n} \mathfrak{a}_i \xrightarrow{\sim} R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$$

induziert.

a) *Zeigen Sie*: Für $j = 1, \ldots, n$ sind die Ideale $\mathfrak{a}_j$ und $\bigcap_{i \neq j} \mathfrak{a}_i$ koprim, d.h. ihre Summe ist gleich R. Insbesondere existieren Gleichungen $d_j + e_j = 1$ mit $d_j \in \mathfrak{a}_j, e_j \in \bigcap_{i \neq j} \mathfrak{a}_i$.

b) *Zeigen Sie*: Es ist
$$\pi_i(e_j) = \begin{cases} 1 & \text{für} \quad i = j \\ 0 & \text{für} \quad i \neq j, \end{cases}$$
d.h. $\varphi(e_j)$ ist der „j-te Einheitsvektor“ in $R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$.

c) *Folgern Sie* aus b) mit Hilfe der Linearität von φ die Surjektivität von φ und den Chinesischen Restsatz.

d) *Erklären Sie*, wie sich für einen Hauptidealring R der Chinesische Restsatz auf die folgende Form spezialisiert: Sei R ein Hauptidealring und $a = \varepsilon p_1^{n_1} \cdots p_r^{n_r}$ eine Primfaktorzerlegung in R mit einer Einheit ε und paarweise nicht-assoziierten Primelementen p_i. Dann ist der Homomorphismus
$$\varphi \colon R \to R/(p_1^{n_1}) \times \ldots \times R/(p_r^{n_r}), \qquad x \mapsto (\pi_1(x), \ldots, \pi_r(x))$$
surjektiv und erfüllt $\ker(\varphi) = (a)$, induziert also einen Isomorphismus
$$R/(a) \xrightarrow{\sim} R/(p_1^{n_1}) \times \ldots \times R/(p_r^{n_r}).$$

Bemerkung: Der Beweis des Chinesischen Restsatzes liefert ein praktisches Verfahren zur Lösung simultaner Kongruenzen in einem euklidischen Ring, weil man Elemente $d_j \in (p_j^{n_j})$ und $e_j \in (\prod_{i \neq j} p_i^{n_i})$ mit $d_j + e_j = 1$ unter Verwendung des Euklidischen Algorithmus konstruieren kann.

Aufgabe 4. (4 Punkte). Eine Bande von 25 Piraten besitzt einen Schatz aus gleichwertigen Goldmünzen. Sie planen, sie zu gleichen Teilen zu teilen und den Rest dem chinesischen Koch zu geben. Dieser würde dann 2 Münzen erhalten. Aber die Piraten streiten und 16 von ihnen werden getötet. Ein neuer Anteil würde dem Koch 3 Stück geben. Bei einem späteren Schiffbruch werden nur der Schatz, 8 Piraten und der Koch gerettet, und das Teilen würde diesem dann 4 Gold einbringen. Auf welches Vermögen kann der Koch mindestens hoffen, wenn er beschließt, den Rest der Piraten zu vergiften?